Chapter IV

A Secure Authentication Infrastructure for Mobile Users

Gregor v. Bochmann, University of Ottawa, Canada
Eric Zhen Zhang, University of Ottawa, Canada

Abstract

The requirements for an authentication infrastructure for electronic commerce are explained by identifying the partners involved in e-commerce transactions and the trust relationships required. Related security requirements are also explained, such as authentication, access rights, payment credentials, anonymity (in certain cases), and privacy and integrity of message exchanges. Then several general authentication schemes and specific protocols are reviewed and their suitability for mobile users is discussed. Finally, an improved authentication protocol is presented which can provide trust relationships for mobile e-commerce users. Its analysis and comparison with other proposed authentication protocols indicate that it is a good candidate for use in the context of mobile e-commerce.
Introduction

With the introduction of the World Wide Web, electronic commerce has begun to enhance the traditional commerce practice in the exchange of merchandise and information. Recently, the emergence of wireless networks and mobile devices has introduced further commodities for using telecommunication services and electronic commerce transactions on the go. Mobile commerce may be defined as the exchange or buying and selling of commodities, services or information on the Internet through the use of mobile handheld devices. However, in this chapter we take a little larger view of mobile commerce by including the notion of “mobile users,” which means that the user may be in a foreign country, in an unusual environment and may use, for the electronic commerce session, any device that happens to be available, for instance a workstation in a hotel business lounge or the handheld device belonging to a friend.

While many aspects of mobile commerce are identical to the same aspects of normal electronic commerce, in general, there are certain aspects that are specific to mobile commerce. These aspects are either related to the limitations of handheld devices, such as (a) the limited computation power of most handheld devices related to CPU power and battery life and (b) certain limitations of the communication bandwidth, which depends on the particular wireless networking technology in use, or related to the notion of “mobile users,” such as (c) the security implications of using unknown ad hoc devices that are locally available and (d) the fact that the user may need to be authenticated by a foreign organization that provides network access facilities and other services within the foreign domain where the user temporarily resides.

In this chapter, we principally deal with the problem of user authentication and the establishment of trust relationships between the different parties involved in an electronic commerce transaction. In this context, we consider specifically the aspects (c) and (d) above which are specific to mobile commerce. To a lesser degree we are also concerned with aspect (a) and (b).

In second section, we explain the requirements for an authentication infrastructure for electronic commerce by identifying the partners that are typically involved in transactions and the trust relationships that are required. We also describe the security requirements, such as authentication, access rights, payment credentials, anonymity (in certain cases), as well as the traditional requirements such as privacy and integrity of message exchange. Then we review in the third section the three general schemes for authentication, namely authentication based on a shared key, on public/private key pair, and on biometric information. After this introduction, we review certain authentication protocols that are currently in use or proposed, and discuss their applicability to electronic commerce applications and in particular to the requirements of mobile users as identified by points (c) and (d) above.

In the fourth section, we then propose a secure authentication protocol for mobile user that (1) combines ease of password-based authentication with the power of public key technology, (2) can be executed on an ad hoc device that happens to be available in the environment of the mobile user, and (3) provides authentication support for (i) the normal electronic commerce transactions, (ii) for obtaining the necessary transmission re-
eBay's Dominance in Internet Auctions
www.igi-global.com/chapter/ebay-dominance-internet-auctions/9536?camid=4v1a